

## Association for Information Systems AIS Electronic Library (AISeL)

---

PACIS 2003 Proceedings

Pacific Asia Conference on Information Systems  
(PACIS)

---

December 2003

# Defining Fraud: Issues for Organizations from an Information Systems Perspective

Lucian Vaisu  
*Deakin University*

Matthew Warren  
*Deakin University*

David Mackay  
*Deakin University*

Follow this and additional works at: <http://aisel.aisnet.org/pacis2003>

---

### Recommended Citation

Vaisu, Lucian; Warren, Matthew; and Mackay, David, "Defining Fraud: Issues for Organizations from an Information Systems Perspective" (2003). *PACIS 2003 Proceedings*. 66.  
<http://aisel.aisnet.org/pacis2003/66>

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2003 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# Defining Fraud: Issues for Organizations from an Information Systems Perspective

Lucian Vasiu<sup>a</sup>, Matthew Warren<sup>b</sup> and David Mackay<sup>a</sup>

<sup>a</sup> School of Information Systems, Deakin University  
Geelong, VIC, Australia, 3217  
(lvasi, mackay}@deakin.edu.au

<sup>b</sup> School of Information Technology, Deakin University  
Geelong, VIC, Australia, 3217  
mwarren@deakin.edu.au

## ABSTRACT

*Fraud is one of the besetting evils of our time. While less dramatic than crimes of violence like murder or rape, fraud can inflict significant damage at organizational or individual level.*

*Fraud is a concept that seems to have an obvious meaning until we try to define it. As fraud exists in many different guises, and it is necessary to carefully define what it is and to tailor policies and initiatives accordingly.*

*Developing a definition of fraud is an early step of a prevention program. In order to be involved in the protection function, people at all levels of an organization must be knowledgeable about fraud. In this paper, we discuss the risk of fraud from an information systems perspective, explain what fraud is and present a range of definitions of fraud and computer fraud. We argue that without clearly defining fraud, organizations will not be able to share information that has the same meaning to everyone, to agree on how to measure the problem, and to know the extent of the problem, in order to decide how much and where to deploy resources to effectively solve it.*

## Keywords

Fraud, computer fraud, information systems.

## Introduction

Fraud is one of the besetting evils of our time. While no one knows the exact extent of fraud, it hardly passes a day without some reference in the media to yet another fraud or alleged fraud.

Viewed as a victimless crime, fraud does not draw community and political reaction like other crimes (Chapman & Smith 2001). Yet, while less dramatic than crimes of violence like murder or rape, many now believe that fraud can be as serious or even more serious than certain types of street crimes (Rebovich & Kane 2002).

Fraud can inflict significant damage at community, organizational or individual level (Lanham, Weinberg, Brown & Ryan 1987), and the potential consequences of fraud for

organizations can be strategic, legal, financial or operational. Therefore, it must be an important issue for organizations.

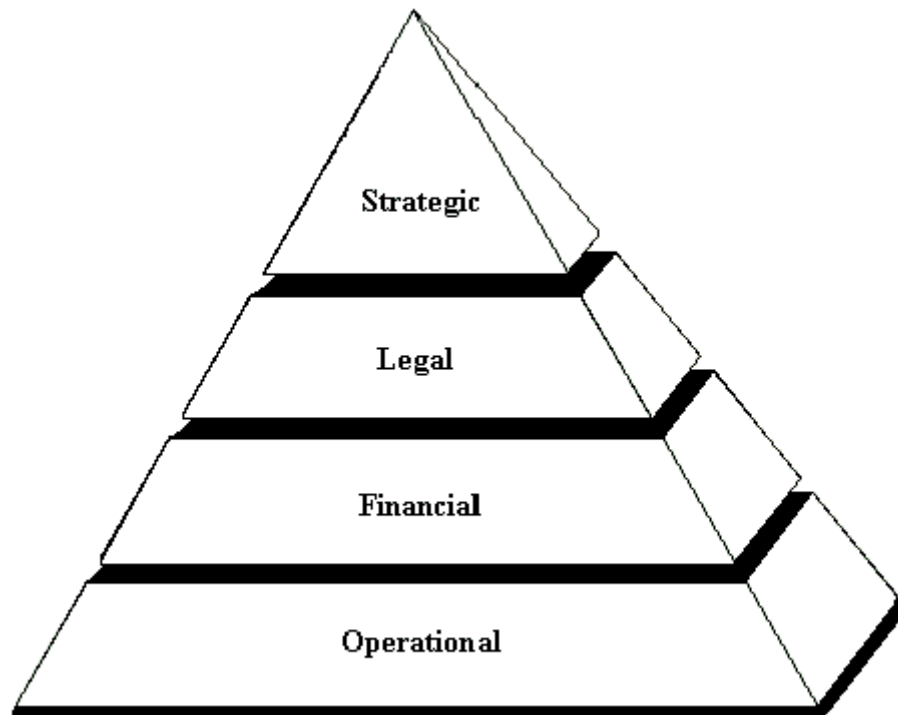


Figure 1. Pyramid of potential consequences of fraud for organizations

In this paper, we argue that without clearly defining fraud, organizations will not be able to share information that has the same meaning to everyone, to agree on how to measure the problem, and to know the extent of the problem, in order to decide how much and where to deploy resources to effectively solve it.

The rationales for this paper are:

- ❑ Frauds are highly destructive to free-market capitalism and, more broadly, to the underpinnings of society (Greenspan 2002). In order to be involved in the protection function, people at all levels of an organization must be knowledgeable about fraud.
- ❑ Clearly defining fraud is a step toward sharing information that has the same meaning to everyone.

This paper is structured as follows. In the next section, we look into the risk of fraud associated with computerized information systems and discuss the act of fraud in general. Next, we present and comment a range of fraud definitions: dictionary definitions, scholar definitions, organization definitions and legal definitions of computer fraud. Finally, we draw our conclusions.

## Fraud and Information Systems

Al Capone's bookkeeper once said (quoted in Brinkley and Schell in Abrams, Jajodia & Podell 1995) that he can steal more with a pencil than ten men with machine guns—the situation is much worse today, with computers that have increased the speed, the possible scope of criminal acts and the difficulty to investigate such crimes. Furthermore, money in electronic form are much easier to steal: while US\$1B in \$100 bills occupies about 15 cubic

meters, and in gold would weigh about 65 tons, in electronic form is just 32 bits plus some application-dependent headers (Parker 1998).

People may not be any greedier than in generations past, however the avenues to express greed had grown enormously (Greenspan 2002). The use of information and communication technology brings many benefits for organizations. The increasing globalisation and range of services the Web technological platform supports (Chatterjee, Grewal & Sambamurthy 2002) offer nearly unimaginable opportunities for organizations in terms of access, speed and choices. Further, corporate billing, payroll or inventory tracking are delivered as services through Internet/web browsers. Yet, along with benefits, there are many risks.

The fundamental principle of criminology is that crime follows opportunity (Grabosky, Smith & Dempsey 2001), and opportunities for fraud abound in today's world. The proliferation of computer systems and other related technologies, and the speed of change, created many opportunities for organizations, however, concomitant, they created widespread vulnerabilities that every organization should be aware of.

Information systems risks are usually classified into accidental and intentional. The foremost intentional risk is the risk of fraud. The ability to edit, alter or otherwise manipulate computerized data to derive benefit from its misrepresentation in a way that is often undetectable increases significantly the fraud opportunities (Smedinghoff 1996). Furthermore, networked computers have lowered the level of expertise required to commit fraud and made it a borderless phenomenon. Fraudsters are able to target a wide range of potential victims throughout the world. *All our lauded technological progress—our very civilization—is like the axe in the hand of the pathological criminal* (Einstein quoted in Casey, 2000).

## What is Fraud?

Where a person obtains property with the consent of the person to whom it belongs, it may seem that there is no offence committed. However, if the property is obtained by improper means we can talk about fraud.

Fraud is not limited to the criminal context. For example, one can find references to fraud in contract and tort law (Podgor 1999). In its widest sense, fraud is a term that has never been consistently and exhaustively defined, and this is not limited to issues of conduct, but also can be seen when the term is used to describe the *mens rea*.

Fraud is a concept that seems to have a perfectly obvious meaning until we try to define it. Fraud is a deep concept, and few use common definitions. Arlidge and Parry (1996) argues that there is a bewildering variety of offences that might be committed in the course of what a layman or a lawyer would describe as a fraud.

*The difficulty of giving an adequate definition of fraud has been felt at all times* (Stephen 1883, p. 1.28). There has always been a great reluctance amongst lawyers to attempt to define fraud, and this is very natural when we consider the number of different kinds of conduct to which this word is applied (Stephen 1883).

All too often fraud is confused with other activities (e.g. theft or espionage). Fraud differs from theft in that the fraud's victim voluntarily parts with his or her property, but does so

because she has been deceived by material false representations made by the fraudster (Brenner 2001). In theft offences, the perpetrator takes someone's property without the victim's permission (or even knowledge).

Fraud is always intentional, intentional by appearance, or intentional by inference from the act. According to Brenner (2001), someone commits fraud if the following four elements are proved beyond a reasonable doubt:

- *Actus reus*: The perpetrator communicates false statements to the victim;
- *Mens rea*: The perpetrator communicates what she knows are false statements with the purpose of defrauding the victim;
- Attendant circumstances: The perpetrator's statements are false; and
- Harm: The victim is defrauded out of property or something of value.

Intent should not be confused with motive, which is what prompts a person to act. Intent refers only to the state of mind with which the act is done. There is no scientific measurement or yardstick for gauging a person's intention, and an inference has to be drawn from all available evidence as to what was in the offender's mind at the material time (Justice Ackner in Goldstein, Dershowitz & Swartz 1974).

The element of the intent to defraud connotes the intention to produce a consequence that is in some sense detrimental to a lawful right, interest, opportunity or advantage of the person to be defrauded, and is an intention distinct from and additional to the intention to use the forbidden means (King CJ in Waller and Williams 2001).

Fraud is not a crime in itself in certain jurisdictions, however, it is an integral aspect of several criminal statutes. In legal terms, fraud is a generic category of criminal conduct that involves the use of dishonest or deceitful means in order to obtain an unfair advantage or gain over another, in order to secure something of value or deprive another of a right (Smith 2001).

In the following section, we present a range of definitions of fraud: dictionary definitions, scholar definitions, organization definitions and legal definitions of computer fraud.

## Definitions of Fraud and Computer Fraud

### Preliminary considerations

A major purpose of a definition is to ensure consistency and common understanding across organizations, to facilitate communication and promote shared usage of terms. A definition must be certain and consistent, so that responses may be foreseen, and practical, so that is effective means of handling actualities (Goldstein *et al.* 1974).

Fraud comes in all shapes and sizes, large and complex, small and simple, and anything in between (Kirk & Woodcock 1992). Fraud has an incredible breadth and encompasses everything from expense account and procurement scams to financial reporting irregularities, bid-rigging, intellectual property theft and much more. Furthermore, specific financial-service sector industries such as insurance or banking have their own unique strains of fraud to worry about (Duffy 2003).

Fraud definitions are not universal, and can only be understood in the cultural context in which they occur. Moreover, fraud can be committed for the benefit of the organization, or there can be situations when one is not stealing for him, however he may robbing from one client to feed the other (Cohen 2002), or may not cause a loss to organization while defrauding its customers (e.g. salami attacks).

Developing a definition of fraud is an early step of a fraud prevention program. Fraud boasts many different guises, and it is necessary to carefully define what it is and to tailor policies and initiatives accordingly (Smith 2001). In the following section, we present a range of fraud definitions that can be used by organizations in the process of defining what fraud is from their perspective.

## Dictionary definitions

The term “fraud” is defined in Gilbert (1997, p. 124) as

*An act using deceit such as intentional distortion of the truth of misrepresentation or concealment of a material fact to gain an unfair advantage over another in order to secure something of value or deprive another of a right. Fraud is grounds for setting aside a transaction at the option of the party prejudiced by it or for recovery of damages.*

Merriam-Webster (2003) defines “fraud” as

*1 a : Deceit, trickery; specifically : intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right b : an act of deceiving or misrepresenting : Trick  
2 a : a person who is not what he or she pretends to be : Impostor; also : one who defrauds : Cheat b : one that is not what it seems or is represented to be.*

## Scholar definitions

The classic scholar definition is Stephen’s (1883, p. II.121):

*I shall not attempt to construct a definition which will meet every case which might be suggested, but there is little danger in saying that whenever the words ‘fraud’ or ‘intent to defraud’ or ‘fraudulently’ occur in the definition of a crime two elements at least are essential to the commission of the crime: namely, first, deceit or an intention to deceive or in some cases mere secrecy; and, secondly, either actual injury or possible injury or an intent to expose some person either to actual injury or to a risk of possible injury of that deceit or secrecy.*

According to Smith (2001, pp. 1-2),

*In legal terms, fraud is a generic category of criminal conduct that involves the use of dishonest or deceitful means in order to obtain some unjust advantage or gain over another.*

*In business terms, fraud is sometimes difficult to define as it extends, for example, from conduct as trivial as an employee having an extended lunch break without permission, to large-scale misappropriation of funds by a company accountant involving many millions of dollars.*

Zervos argues (1992, p. 199) that,

*In simple terms, fraud is the art of deception for gain. Dishonesty is an essential ingredient. Fraud varies in type, size and complexity. It is encountered in many*

*different contexts. It is very much a creature of its time; it changes as society changes, with all its different attitudes and technological advancements.*

## Organizations definitions

Definitions of fraud vary between organizations and countries. In the Australian Government's Fraud Control Policy (Commonwealth of Australia 2000), "fraud" is described as

*Inducing a course of action by deceit or other dishonest conduct, involving acts or omissions or the making of false statements, orally or in writing, with the object of obtaining money or other benefit from, or of evading a liability to, the Commonwealth.*

The Government of Western Australia (1999, p. 9) takes a broad view and includes non monetary benefits, such as misusing company time or assets:

*Any practice that involves deceit or other dishonest means by which a benefit is obtained from the government.*

## Legal definitions of computer fraud

Some (e.g. Ernst & Young 2002) argue that there is no such thing as computer fraud, and what is usually meant by computer fraud is fraud carried out using a computer, rather than traditional methods of paper and pen. However, computers increased significantly the fraud problem in that users, from remote locations, can access computers to further frauds, and the detection and policing of computer frauds is very difficult and expensive (Etter 2001; Varney 2000; McKemmish 1999).

In general, the definitions of computer fraud make it illegal to commit fraud using a computer and will consists of the following elements:

- ❑ The intent to defraud;
- ❑ The access to a protected computer without authorization, or abusing authorization, and
- ❑ The furtherance of a fraud.

The U.S. Computer Fraud and Abuse Act (18 U.S.C. 1030) defines (a)(4) "computer fraud" as:

*(a) Whoever... (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period...*

We should note the very broad language used—this intends to tackle new types of frauds before particularized legislation is developed—, and that this definition may seems circular to non-lawyers. It clearly is not circular in a legal sens, however, to give insight into what frauds can be perpetrated, we considered useful to include Virginia's definition of computer fraud (§ 18.2-152.3)

*Any person who uses a computer or computer network without authority and with the intent to:*

- 1. Obtain property or services by false pretenses;*
- 2. Embezzle or commit larceny; or*

*3. Convert the property of another shall be guilty of the crime of computer fraud. If the value of the property or services obtained is \$200 or more, the crime of computer fraud shall be punishable as a Class 5 felony. Where the value of the property or services obtained is less than \$200, the crime of computer fraud shall be punishable as a Class 1 misdemeanor.*

Another useful definition is Council of Europe's (2001), in that it gives us insight into the criminal activity. According to this definition, computer-related fraud is

*The causing of a loss of property to another by:*

- *any input, alteration, deletion or suppression of computer data,*
- *any interference with the functioning of a computer system,*
- with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.*

## Conclusions

Fundamental changes in information systems and the heavy dependence on computers increased significantly the risk of fraud. While no genuinely new frauds are expected, *electronic variations of traditional frauds will be carried out with greater efficiency and effectiveness, will have potentially greater impact and will be more difficult to investigate* (Wardlaw, 1999, p. 8). The latter is due to the fact that a sophisticated fraud might leave no evidence of how and when it occurred, there will be no collateral or forensic evidence such as eyewitnesses, fingerprints or DNA (Etter 2001), and because the offender and victim may be located thousands of miles apart.

The very stealth of fraud avoids attention, yet it can inflict significant damage at organizational or individual level. Fraud is not just a criminal offence—it is a major social problem. Fraud is growing worldwide and is becoming more costly to businesses every year (Farrell & Healy 2000) as offenders use sophisticated techniques to perpetrate and mask their crimes.

The primary costs of fraud are obvious, however, potentially secondary costs may be equally harmful:

- ❑ Diminished faith in the organization,
- ❑ Loss of stakeholders confidence and market valuation, and
- ❑ Erosion of public morality.

It is essential for organizations to have policies in place that define fraud, as part of change management, in such a way as to facilitate operational risk management. Organizations need to define which types of conduct they are seeking to prevent (Smith 2001), to avoid any ambiguities. Furthermore, without clearly defining fraud, organizations will not be able to share information that has the same meaning to everyone, to agree on how to measure the problem, to know the extent of the problem, in order to know how much and where to deploy resources to effectively solve it.

## References

- Abrams, MD, Jajodia, S & Podell, HJ (1995), *Information security: An integrated collection of essays*, IEEE Computer Society Press, Los Alamitos, CA.
- Arlidge, AJ & Parry, J (1996), *Fraud*, Sweet and Maxwell, London.



- Brenner, SW (2001), 'Is There Such a Thing as "Virtual Crime"?' in 4 *California Criminal Law Review* 1.
- Casey, E (2000), *Digital evidence and computer crime: Forensic science, computers and the Internet*, Academic Press.
- Chapman, A & Smith, RG (2001), 'Controlling Financial Services Fraud' in *Trends and Issues in Crime and Criminal Justice*, No. 189, Australian Institute of Criminology, Canberra.
- Chatterjee, D, Grewal, R & Sambamurthy V (2002), 'Shaping Up for E-Commerce: Institutional Enablers of the Organizational Assimilation of Web Technologies' in *MIS Quarterly*, vol. 26, no. 2, June 2002, pp. 65-89.
- Cohen, F (2002), 'Computer Fraud Scenarios: Robbing the Rich to Feed the Poor' in *Computer Fraud & Security*, vol. 2002, iss. 1, December, pp. 5-6.
- Commonwealth of Australia (2000), *The Changing Nature of Fraud in Australia*, URL: <http://www.law.gov.au/publications/Fraud.htm>, Last accessed: 1 September, 2001.
- Council of Europe (2001), *Final Draft Convention on Cyber-crime*, URL: <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>, Last Accessed: 1 August, 2002.
- Duffy, D (2003), 'The fraud squad' in *CSO Magazine*, January.
- Ernst & Young (2002), *Fraud risk and prevention*.
- Etter, B (2001), 'The forensic challenges of e-crime' in *7th Indo-Pacific Congress on Legal Medicine and Forensic Sciences*, Melbourne, Australia.
- Farrell, BR & Healy, P (2000), 'White Collar Crime: A Profile of the Perpetrator and an Evaluation of the Responsibilities for its Prevention and Detection' in *Journal of Forensic Accounting*, vol. I, pp. 17-34.
- Gilbert (1997), *Law Dictionary*, Harcourt Brace Legal and Professional Publications.
- Goldstein, J, Dershowitz, AM & Swartz, RD (1974), *Criminal law: Theory and process*, The Free Press, New York.
- Government of Western Australia (1999), *Fraud prevention in Western Australian public sector*, URL: <http://www.dpc.wa.gov.au/psmd/pubs/psrd/governance/fraud2.pdf>, Last accessed: 1 February 2003.
- Grabosky, P, Smith, RG & Dempsey, G (2001), *Electronic theft: Unlawful acquisition in cyberspace*, Cambridge University Press.
- Greenspan, A (2002), *Monetary Policy Report to the Congress*, July 16, 2002.
- Kirk, DN & Woodcock, AJJ (1992), *Serious fraud: investigation and trial*, Butterworths.
- Lanham, D, Weinberg, M, Brown, KE & Ryan, GW (1987), *Criminal fraud*, The Law Book Company Limited.
- McKemmish, R (1999), 'What is forensic computing?' in *Trends and Issues No. 118*, Australian Institute of Criminology.
- Merriam-Webster (2003), *OnLine Dictionary*, URL: <http://www.webster.com>, Last accessed: 1 February, 2003.

- Parker, BD (1998), *Fighting Computer Crime: A New Framework for Protecting Information*, John Willey & Sons, Inc.
- Podgor, ES (1999), 'Criminal Fraud' in *American University Law Review*, vol. 48, no. 4.
- Rebovich, DJ & Kane JL (2002), 'An eye for an eye in the electronic age: Gauging public attitude toward white collar crime and punishment' in *Journal of Economic Crime Management*, vol. 1, iss. 2, Fall.
- Smith, RG (2001), 'Defining, Measuring, and Reporting Fraud Risk Within Your Organisation' in *Applying Risk Management to Implement a Proactive Fraud Prevention Strategy in Financial Services*, I.I.R. Conferences, Parkroyal Darling Harbour, 19-20 July 2001, URL: [http://www.aic.gov.au/conferences/other/smith\\_russell/2001-07-IIR.pdf](http://www.aic.gov.au/conferences/other/smith_russell/2001-07-IIR.pdf), Last accessed: 1 February, 2003.
- Smedinghoff, TJ (1996), *Online Law, The SPA's Legal Guide to Doing Business on the Internet*, Addison-Wesley Developers Press.
- Stephen, JF (1883), *A history of the Criminal Law of England*, vols. I-III, Macmillan and Co. (reprinted by William S. Hein & Co., Inc., Buffalo, New York).
- Varney, T (2000), 'Computer forensics' in *Internal Auditing*, November/December, pp. 31-33.
- Waller, L & Williams, CR (2001), *Criminal law: Text and cases*, 9<sup>th</sup> Ed., Butterworths, Australia.
- Wardlaw, G (1999), 'The future and crime: challenges for law enforcement' in *3<sup>rd</sup> National Outlook Symposium on Crime in Australia*, Canberra, 22-23 March.
- Zervos, K (1992), 'Responding to Fraud in the 1990s' in *Complex Commercial Fraud: Proceedings of a Conference*, 20-23 August 1991, Edited by Grabosky, P. N., Canberra, Australian Institute of Criminology Conference Proceedings, No. 10, pp. 199-209.